

## PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-023137

(43)Date of publication of application : 21.01.2000

(51)Int.Cl.

H04N 7/167

H04H 1/00

H04L 9/08

H04L 9/14

(21)Application number : 10-201090

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD

(22)Date of filing : 02.07.1998

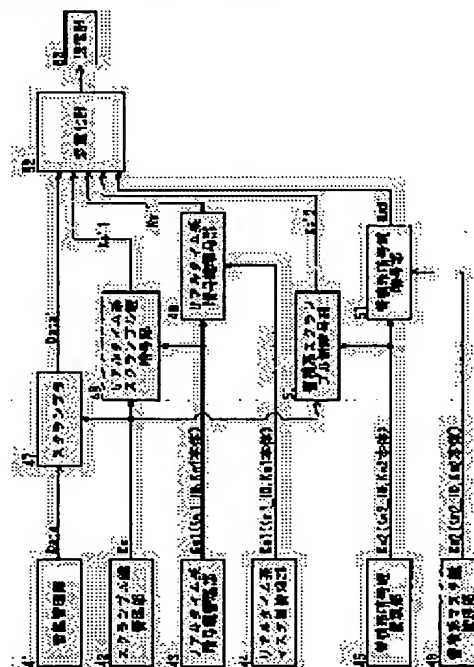
(72)Inventor : MASUDA ISAO  
GOTO YOSHIMASA  
HARADA TAKENOSUKE  
MACHIDA KAZUHIRO  
KATAOKA MITSUTERU

## (54) BROADCASTING SYSTEM AND BROADCASTING TRANSMITTER- RECEIVER

## (57)Abstract:

PROBLEM TO BE SOLVED: To provide a broadcasting system capable of preventing the fraudulent viewing of stored program data.

SOLUTION: In this broadcasting system by which a program is broadcasted on the side of transmission, the program is viewed on the side of reception in real time or stored, reproduced later and viewed, a scramble key 42 for descrambling program data 451 is transmitted on the side of transmission while being enciphered through plural kinds of cryptographic keys 43 and 45 at different updating intervals by enciphering parts 48 and 50, and when storing the broadcasting program, on the side of reception, the scrambled program data are stored corresponding to the scramble key enciphered by the cryptographic key at short updating intervals. Even when the cryptographic key is fraudulently deciphered, the condition of viewing all the stored programs can be prevented.



## LEGAL STATUS

[Date of request for examination]

21.02.2001

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

3565715

[Date of registration] 18.06.2004

[Number of appeal against examiner's decision  
of rejection]

[Date of requesting appeal against examiner's  
decision of rejection]

[Date of extinction of right]

Copyright (C); 1998,2003 Japan Patent Office

(11)特許出願公開番号

特開2000-23137

(P2000-23137A)

(43)公開日 平成12年1月21日(2000.1.21)

(51)Int.Cl.'	識別記号	F I	テマコード*(参考)
H 0 4 N 7/167		H 0 4 N 7/167	5 C 0 6 4
H 0 4 H 1/00		H 0 4 H 1/00	F 5 K 0 1 3
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 A
9/14			6 4 1

審査請求 未請求 請求項の数18 FD (全 13 頁)

(21)出願番号	特願平10-201090	(71)出願人	000005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22)出願日	平成10年7月2日(1998.7.2)	(72)発明者	増田 功 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(72)発明者	後藤 吉正 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(74)代理人	100099254 弁理士 役 昌明 (外3名)

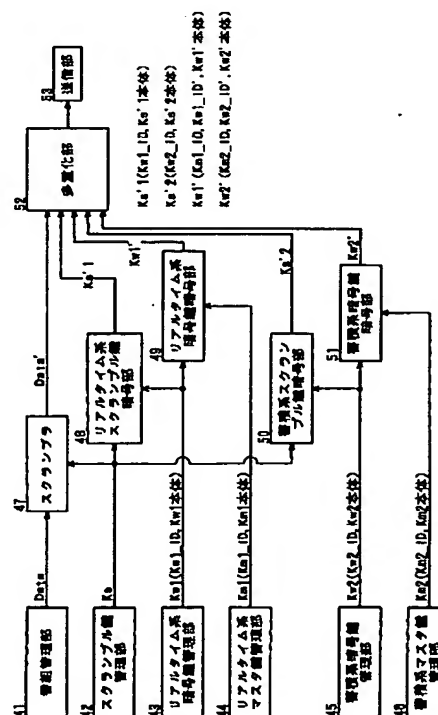
最終頁に続<

(54) 【発明の名称】 放送システムと放送送受信装置

(57) 【要約】

【課題】 蓄積された番組データの不正視聴を防ぐこと  
ができる放送システムを提供する。

【解決手段】 送信側が番組を放送し、受信側が、この番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムにおいて、送信側では、番組データ41のスクランブルを解くスクランブル鍵42を、更新間隔を異にする複数種類の暗号鍵43、45で暗号部48、50で暗号化して送信し、受信側では、放送番組を蓄積するとき、スクランブルされた番組データと、更新間隔が短い暗号鍵で暗号化されたスクランブル鍵とを対応付けて蓄積する。暗号鍵が不正に解かれた場合でも、蓄積されている番組の全てが視聴可能になってしまう事態を防ぐことができる。



## 【特許請求の範囲】

【請求項1】 送信側が番組を放送し、受信側が、この番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムにおいて、

送信側では、番組データのスクランブルを解くスクランブル鍵を複数種類の暗号鍵で暗号化し、前記暗号鍵の各々を暗号化して送信し、

受信側では、暗号化された複数種類の暗号鍵を復号化して保持し、蓄積した番組を再生して視聴する場合に、リアルタイムで番組を視聴するときに用いる暗号鍵とは異なる暗号鍵を用いて蓄積されたスクランブル鍵を復号化し、復号化した前記スクランブル鍵を用いて蓄積された番組データのスクランブルを解除することを特徴とする放送システム。

【請求項2】 送信側では、前記複数種類の暗号鍵の更新間隔を違えて、暗号化した前記複数種類の暗号鍵を送信し、受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵より更新間隔が短い暗号鍵を、蓄積した番組の視聴のために用いることを特徴とする請求項1に記載の放送システム。

【請求項3】 送信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を第1の種類のマスタ鍵で暗号化し、蓄積した番組を視聴するときに用いる暗号鍵を第2の種類のマスタ鍵で暗号化することを特徴とする請求項1または2に記載の放送システム。

【請求項4】 送信側では、蓄積した番組を視聴するときに用いる前記暗号鍵を番組ごとに更新することを特徴とする請求項2または3に記載の放送システム。

【請求項5】 受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を前記第1の種類のマスタ鍵で復号化して保持し、放送番組をリアルタイムで視聴するときには、復号化した前記暗号鍵を用いて、暗号化されたスクランブル鍵を復号化し、復号化した前記スクランブル鍵を用いて番組データのスクランブルを解除することを特徴とする請求項1乃至4に記載の放送システム。

【請求項6】 受信側では、蓄積した番組を視聴するときに用いる暗号鍵を前記第2の種類のマスタ鍵で復号化して保持し、蓄積した番組を再生して視聴するときには、復号化した前記暗号鍵を用いて、蓄積されている暗号化されたスクランブル鍵を復号化し、復号化した前記スクランブル鍵を用いて再生する番組データのスクランブルを解除することを特徴とする請求項1乃至4に記載の放送システム。

【請求項7】 送信側では、前記第2の種類のマスタ鍵を前記第1の種類のマスタ鍵で暗号化して送信することを特徴とする請求項3に記載の放送システム。

【請求項8】 受信側では、暗号化されて送られて来る前記第2の種類のマスタ鍵を前記第1の種類のマスタ鍵で復号化して保持することを特徴とする請求項7に記載の放送システム。

【請求項9】 前記第1の種類のマスタ鍵が、各受信側に個別に設定され、前記第2の種類のマスタ鍵が、各受信側に共通に設定されることを特徴とする請求項3、5、6、7または8に記載の放送システム。

【請求項10】 受信側が放送番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの送信装置において、

第1の種類の暗号鍵を生成管理する第1の暗号鍵管理手段と、

10 第2の種類の暗号鍵を生成管理する第2の暗号鍵管理手段と、

番組データを暗号化したスクランブル鍵を、前記第1の種類の暗号鍵で暗号化する第1のスクランブル鍵暗号化手段と、

番組データを暗号化したスクランブル鍵を、前記第2の種類の暗号鍵で暗号化する第2のスクランブル鍵暗号化手段と、

前記第1の種類の暗号鍵を第1の種類のマスタ鍵で暗号化する第1の暗号鍵暗号化手段と、

20 前記第2の種類の暗号鍵を第2の種類のマスタ鍵で暗号化する第2の暗号鍵暗号化手段と、

第1のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第2のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第1の暗号鍵暗号化手段で暗号化された暗号鍵、第2の暗号鍵暗号化手段で暗号化された暗号鍵、及びスクランブル鍵で暗号化された番組データを多重化して送信する送信手段とを備えることを特徴とする送信装置。

【請求項11】 前記第2の暗号鍵管理手段が生成管理する第2の種類の暗号鍵の更新期間が、前記第1の暗号鍵管理手段が生成管理する第1の種類の暗号鍵の更新期間より短いことを特徴とする請求項10に記載の送信装置。

【請求項12】 前記第2の種類のマスタ鍵を前記第1の種類のマスタ鍵で暗号化するマスタ鍵暗号化手段を具備し、前記マスタ鍵暗号化手段で暗号化されたマスタ鍵を前記送信手段を通じて送信することを特徴とする請求項10に記載の送信装置。

【請求項13】 前記第1の種類のマスタ鍵を各受信装置ごとに設定し、前記第2の種類のマスタ鍵を各受信装置に共通に設定することを特徴とする請求項10または12に記載の送信装置。

【請求項14】 送信装置から放送された番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの受信装置において、

暗号化されている第1の種類の暗号鍵を、第1の種類のマスタ鍵を用いて復号化する第1の暗号鍵復号手段と、暗号化されている第2の種類の暗号鍵を、第2の種類のマスタ鍵を用いて復号化する第2の暗号鍵復号手段と、

50 スクランブル鍵で暗号化された番組データと前記第2の

種類の暗号鍵で暗号化されたスクランブル鍵とを記憶する蓄積手段と、

前記第1の暗号鍵復号手段で復号化された暗号鍵を用いて、現在の受信情報に含まれる暗号化されたスクランブル鍵を復号化する第1のスクランブル鍵復号手段と、

前記第2の暗号鍵復号手段で復号化された暗号鍵を用いて、前記蓄積手段から読み出した暗号化されているスクランブル鍵を復号化する第2のスクランブル鍵復号手段と、

前記第1のスクランブル鍵復号手段または第2のスクランブル鍵復号手段で復号化されたスクランブル鍵を用いて番組データをデスクランブルするデスクランブラとを備えることを特徴とする受信装置。

【請求項15】 前記第2の暗号鍵復号手段で復号化される第2の種類の暗号鍵の更新期間が、前記第1の暗号鍵復号手段で復号化される第1の種類の暗号鍵の更新期間より短いことを特徴とする請求項14に記載の受信装置。

【請求項16】 前記デスクランブラが、番組をリアルタイム視聴するときには、現在受信しているスクランブルされている番組データを、前記第1のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルし、蓄積された番組を再生して視聴するときには、前記蓄積手段から読み出したスクランブルされている番組データを、前記第2のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルすることを特徴とする請求項14に記載の受信装置。

【請求項17】 暗号化されている前記第2の種類のマスタ鍵を、前記第1の種類のマスタ鍵を用いて復号化するマスタ鍵復号手段を具備し、前記マスタ鍵復号手段で復号化されたマスタ鍵を保持することを特徴とする請求項14に記載の受信装置。

【請求項18】 前記第1の種類のマスタ鍵が、各受信装置ごとに設定され、前記第2の種類のマスタ鍵が、各受信装置に共通に設定されることを特徴とする請求項14または17に記載の受信装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、受信側での放送番組の蓄積を可能にした放送システムと、このシステムで使用する放送受信装置に関し、特に、蓄積した番組の不正視聴を防止するものである。

【0002】

【従来の技術】有料放送では、スクランブルを掛けた番組が放送され、受信契約が有効な場合に、受信装置でスクランブルを解除するデスクランブルが可能となる。

【0003】有料放送での暗号化は、3種類の鍵を用いて行なわれる。番組の映像音声情報はスクランブル鍵(Ks)でスクランブルされ、このスクランブル鍵が暗号鍵(Kw)で暗号化される。また、暗号鍵はマスター

鍵(Km)で暗号化されて受信装置に送信される。

【0004】スクランブル鍵(Ks)は1秒程度の短い周期で更新される各受信装置に共通の鍵である。また、暗号鍵(Kw)は各受信装置に個別に割り当てられる鍵であり、受信契約が交わされると、この暗号鍵がマスター鍵で暗号化されて放送局から受信装置に送信され、また、約1年ごとの受信契約の更新に合わせて、新たな暗号鍵がマスター鍵で暗号化されて放送局から受信装置に送信される。

【0005】マスター鍵(Km)は、受信装置ごとに異なり、各受信装置のセキュリティモジュールに記憶されている。このセキュリティモジュールは、こうした暗号解読用の鍵などの秘密情報や個人IDなどを記憶するICカードで構成され、放送局から送られて来たものが受信装置にセットされる。

【0006】従来の送信装置は、図5に示すように、番組データ(Data)を生成し管理する番組管理部11と、Dataを暗号化するためのスクランブル鍵Ksを生成し管理するスクランブル鍵管理部12と、Ksを暗号化するための暗号鍵Kwを、その識別子(Kw\_ID)と共に生成管理する暗号鍵管理部13と、Kwを暗号化するためのマスタ鍵Kmを、その識別子(Km\_ID)と共に生成し管理するマスタ鍵管理部14と、DataをKsでスクランブルし、スクランブル化された番組データData'を出力するスクランブラ15と、Kwの鍵本体を使ってKsを暗号化し、暗号化スクランブル鍵Ks'を出力するスクランブル鍵暗号部16と、Kmの鍵本体を使ってKwを暗号化し、暗号化暗号鍵Kw'を出力する暗号鍵暗号部17と、Data'、Ks'及びKw'を多重化し、多重化情報として出力する多重化部18と、多重化情報を伝送情報に変換して送信する送信部19とを備えている。

【0007】この装置では、番組管理部11で生成されたDataが、スクランブラ15でスクランブル鍵Ksを使ってスクランブルされ、スクランブル化された番組データData'が多重化部18に出力される。また、このKsは、暗号鍵管理部13で生成されたKwで暗号化される。

【0008】暗号鍵管理部13では、生成する暗号鍵の識別子Kw\_IDと、2byte長のビット配列で、Kw本体を一意に示す値を割り当て、暗号鍵をKw(Kw\_ID、Kw本体)の形式で生成管理している。

【0009】スクランブル鍵暗号部16は、Dataのスクランブルで用いたKsを、暗号鍵管理部13から出力されたKwの鍵本体を使って暗号化し、暗号化に用いたKwのKw\_IDを付加して、暗号化スクランブル鍵をKs'(Kw\_ID、Ks'本体)の形式で多重化部18に出力する。また、このKwは、マスタ鍵管理部14で生成されたKmで暗号化される。

【0010】マスタ鍵管理部14では、生成したマスタ鍵を、識別子と共に、Km(Km\_ID、Km本体)の形式で管理している。

【0011】暗号鍵暗号部17は、契約の更新時期に、Kmの鍵本体を使ってKw(Kw\_ID、Kw本体)を暗号化し、暗号化に用いたKmのKm\_IDを付加して、暗号化暗号鍵をKw'(Km\_ID、Kw\_ID'、Kw'本体)の形式で多重化部18に出力する。

【0012】多重化部18は、入力するData'、Ks'(Kw\_ID、Ks'本体)及びKw'(Km\_ID、Kw\_ID'、Kw'本体)を多重化して、その多重化情報を送信部19に出力し、送信部19は、それを伝送情報に変換して送信する。

【0013】一方、受信装置は、契約時またはその更新時に送られてくる暗号化された暗号鍵を、マスタ鍵で復号化して保持し、この暗号鍵を用いて、暗号化されているスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて番組の映像音声情報のデスクランブルを行なう。

【0014】ところで、特開平10-11894公報や特開平8-149449公報には、放送番組のリアルタイムでの視聴が可能であるとともに、放送番組を蓄積し、都合の良いときに再生して視聴できる放送システムが提案されている。

【0015】こうしたシステムの場合、受信装置で放送番組をリアルタイムで視聴するときには、通常の受信の場合と同様に、受信契約が有効であれば、有料番組のスクランブルは解除され、受信契約が無効であれば、スクランブルは解除されない。また、蓄積された番組を視聴するときも同じであって、その視聴時点で受信契約が有効であれば、視聴する有料番組のスクランブルは解除され、受信契約が無効であれば、スクランブルは解除されない。

【0016】この受信装置の構成を図6に示している。この装置は、受信した伝送情報を多重情報に変換して出力するチューナー21と、チューナー21から出力された多重化情報を暗号化番組データData'、暗号化スクランブル鍵Ks'及び暗号化暗号鍵Kw'に分離して出力する分離部22と、Data'を蓄積する番組データ蓄積部24とKs'を蓄積するスクランブル鍵蓄積部25とを具備する蓄積媒体36と、分離部22で分離されたData'とKs'とを対応をとって番組データ蓄積部24及びスクランブル鍵蓄積部25に書き込む書き込み管理部23と、蓄積されているData'とKs'とを番組データ蓄積部24及びスクランブル鍵蓄積部25から取り出して出力する読み込み管理部26と、リアルタイムで視聴するときは分離部22からData'を選択し、蓄積された番組を視聴するときは読み込み管理部26からData'を選択する番組データ選択部27と、リアルタイムで視聴するときは分離部22からKs'を選択し、蓄積された番組を視聴するときは読み込み管理部26からKs'を選択するスクランブル鍵選択部28と、マスタ鍵Kmを蓄積しているマスタ鍵蓄積部30と、Kmを使ってKw'を復号化し、復号化されたKwを出力する暗号鍵復号部29と、暗号鍵復号部29から入力するKwを蓄

積管理する暗号鍵管理部31と、スクランブル鍵選択部28から入力するKs'を暗号鍵管理部31から取り出したKwで復号化するスクランブル鍵復号部32と、番組データ選択部27から入力するData'をスクランブル鍵復号部32から入力するKsで復号化し、復号化したDataを出力するデスクランブラ33と、Dataを再生信号にデコードするデコーダ34と、再生信号に基づいて番組表示を行なう表示装置35とを備えている。また、マスタ鍵蓄積部30、暗号鍵復号部29、暗号鍵管理部31、及びスクランブル鍵復号部32はセキュリティモジュール37に設けられている。

【0017】この受信装置では、分離部22が、チューナー21から入力する多重化情報を、暗号化番組データData'、暗号化スクランブル鍵Ks'(Kw\_ID、Ks'本体)及び暗号化暗号鍵Kw'(Km\_ID、Kw\_ID'、Kw'本体)に分離して出力する。書き込み管理部23は、分離部22から分離されたData'とKs'とを対応をとって蓄積媒体36の番組データ蓄積部24及びスクランブル鍵蓄積部25に書き込む。

【0018】また、暗号鍵復号部29は、マスタ鍵蓄積部30に蓄積されたマスタ鍵Km(Km\_ID、Km本体)と同一のKm\_IDをもつ暗号化暗号鍵Kw'(Km\_ID、Kw\_ID'、Kw'本体)が分離部22から出力されたとき、そのKmを使ってKw'を復号化し、復号化暗号鍵Kw(Kw\_ID、Kw本体)を暗号鍵管理部31に出力する。暗号鍵管理部31は、これを蓄積管理する。

【0019】視聴者からリアルタイムの番組視聴が指示された場合には、番組データ選択部27は、分離部22からData'を入手してデスクランブラ33に出力し、番組データ選択部27と連動するスクランブル鍵選択部28は、分離部22から暗号化スクランブル鍵Ks'(Kw\_ID、Ks'本体)を入手してスクランブル鍵復号部32に出力する。

【0020】スクランブル鍵復号部32は、スクランブル鍵選択部28からKs'(Kw\_ID、Ks'本体)が入力すると、暗号鍵管理部31からKs'と同一のKw\_IDを持つKw(Kw\_ID、Kw本体)を取り出し、それを使ってKs'を復号化する。復号化されたKsはデスクランブラ33に出力され、デスクランブラ33は、このKsを使って番組データ選択部27から入力するData'を復号化し、復号化したDataをデコーダ34に出力する。

【0021】こうして、有料番組のリアルタイムの視聴が可能となる。

【0022】一方、視聴者から蓄積番組の視聴が指示された場合には、読み込み管理部26は、番組データ蓄積部24から、蓄積されている指示された番組のData'を読み出すとともに、そのData'のスクランブルを行なっているKs'(Kw\_ID、Ks'本体)をスクランブル鍵蓄積部25から取り出す。

【0023】番組データ選択部27は、読み込み管理部26からData'を入手してデスクランブラ33に出力し、番組データ選択部27と連動するスクランブル鍵選択部28は、

読み込み管理部26から暗号化スクランブル鍵K s' (Kw\_ID, K s'本体) を入手してスクランブル鍵復号部32に出力する。

【0024】その後の動作は、リアルタイム視聴の場合と同じである。こうして、蓄積された有料番組の視聴が可能となる。

【0025】

【発明が解決しようとする課題】しかし、この蓄積型放送システムでは、暗号鍵K wの更新周期が約1年であるため、受信装置の蓄積媒体36には、同一の暗号鍵K wで暗号化されたスクランブル鍵K s' によりスクランブルされている番組が多数蓄積されることになり、暗号鍵K wが不正に解かれた場合、その暗号鍵で、それらの蓄積されている全ての番組データが不正に視聴できてしまうという問題点を有している。

【0026】この点は、暗号鍵K wの更新周期を短縮すれば解消できるが、しかし、暗号鍵K wを暗号化するマスタ鍵K mは各受信装置ごとに異なっているため、何10万台にも及ぶ受信装置のそれぞれのマスタ鍵K mで暗号鍵K wを暗号化するのに多くの時間が掛かり、短い間隔で暗号鍵K wを更新することは実際上できない。

【0027】本発明は、こうした点の改善を図るものであり、蓄積された番組データの不正視聴を防止する放送システムを提供し、また、その放送システムを実現する放送送信装置と放送受信装置とを提供することを目的としている。

【0028】

【課題を解決するための手段】そこで、本発明の放送システムでは、スクランブル鍵を暗号化する暗号鍵として、複数種類の暗号鍵を用意し、番組をリアルタイムで視聴するときにスクランブル鍵を復号化する暗号鍵と、蓄積した番組を再生して視聴するときにスクランブル鍵を復号化する暗号鍵との種類を違えている。

【0029】また、蓄積した番組を視聴するときに用いる暗号鍵の更新間隔を、リアルタイムで番組を視聴するときに用いる暗号鍵の更新間隔より短く設定している。

【0030】このように、蓄積した番組の視聴に、リアルタイム視聴の場合と異なる種類の暗号鍵を使用し、また、その暗号鍵を短い間隔で更新することにより、暗号鍵が不正に解かれた場合の被害を極小化することができ、蓄積された番組が広く不正視聴されてしまう事態を防止することができる。

【0031】

【発明の実施の形態】本発明の請求項1に記載の発明は、送信側が番組を放送し、受信側が、この番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムにおいて、送信側では、番組データのスクランブルを解くスクランブル鍵を複数種類の暗号鍵で暗号化し、その暗号鍵の各々を暗号化して送信し、受信側では、暗号化された複数種類の暗号鍵を復号化して

保持し、蓄積した番組を再生して視聴する場合に、リアルタイムで番組を視聴するときに用いる暗号鍵とは異なる暗号鍵を用いて蓄積されたスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて蓄積された番組データのスクランブルを解除するようにしたものであり、複数種類の暗号鍵を用いることにより、暗号鍵が不正解読された場合の被害の範囲を狭めることができる。

【0032】請求項2に記載の発明は、送信側では、複数種類の暗号鍵の更新間隔を違えて、暗号化した複数種類の暗号鍵を送信し、受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵より更新間隔が短い暗号鍵を、蓄積した番組の視聴のために用いるようにしたものであり、暗号鍵が不正に解かれた場合でも、蓄積されている番組の全てが視聴可能になってしまう事態を防ぐことができる。

【0033】請求項3に記載の発明は、送信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を第1の種類のマスタ鍵で暗号化し、蓄積した番組を視聴するときに用いる暗号鍵を第2の種類のマスタ鍵で暗号化するようにしたものであり、蓄積番組の視聴に用いる暗号鍵を、リアルタイム視聴に用いる暗号鍵とは異なる態様で暗号化することができる。

【0034】請求項4に記載の発明は、送信側では、蓄積した番組を視聴するときに用いる暗号鍵を番組ごとに更新するようにしたものであり、暗号鍵の1つが不正に解かれた場合でも、蓄積されている他の番組は不正視聴から免れることができる。

【0035】請求項5に記載の発明は、受信側では、リアルタイムで番組を視聴するときに用いる暗号鍵を第1の種類のマスタ鍵で復号化して保持し、放送番組をリアルタイムで視聴するときには、復号化したこの暗号鍵を用いて、暗号化されたスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて番組データのスクランブルを解除するようにしたものであり、リアルタイムでの番組視聴が可能となる。

【0036】請求項6に記載の発明は、受信側では、蓄積した番組を視聴するときに用いる暗号鍵を第2の種類のマスタ鍵で復号化して保持し、蓄積した番組を再生して視聴するときには、復号化したこの暗号鍵を用いて、蓄積されている暗号化されたスクランブル鍵を復号化し、復号化したスクランブル鍵を用いて再生する番組データのスクランブルを解除するようにしたものであり、蓄積された番組の再生視聴が可能となる。

【0037】請求項7に記載の発明は、送信側では、第2の種類のマスタ鍵を、第1の種類のマスタ鍵で暗号化して送信するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて配布することができ、このマスタ鍵を変更することが容易になる。

【0038】請求項8に記載の発明は、受信側では、暗



号化されて送られて来る第2の種類のマスタ鍵を、第1の種類のマスタ鍵で復号化して保持するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて取得することができる。

【0039】請求項9に記載の発明は、第1の種類のマスタ鍵を、各受信側に個別に設定し、第2の種類のマスタ鍵を、各受信側に共通に設定するようにしたものであり、蓄積番組視聴用の暗号鍵が各受信側に共通に設定したマスタ鍵で暗号化されるため、暗号化に多くの時間を必要とせず、更新間隔を短くすることができる。

【0040】請求項10に記載の発明は、受信側が放送番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの送信装置において、第1の種類の暗号鍵を生成管理する第1の暗号鍵管理手段と、第2の種類の暗号鍵を生成管理する第2の暗号鍵管理手段と、番組データを暗号化したスクランブル鍵を第1の種類の暗号鍵で暗号化する第1のスクランブル鍵暗号化手段と、番組データを暗号化したスクランブル鍵を第2の種類の暗号鍵で暗号化する第2のスクランブル鍵暗号化手段と、第1の種類の暗号鍵を第1の種類のマスタ鍵で暗号化する第1の暗号鍵暗号化手段と、第2の種類の暗号鍵を第2の種類のマスタ鍵で暗号化する第2の暗号鍵暗号化手段と、第1のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第2のスクランブル鍵暗号化手段で暗号化されたスクランブル鍵、第1の暗号鍵暗号化手段で暗号化された暗号鍵、第2の暗号鍵暗号化手段で暗号化された暗号鍵、及びスクランブル鍵で暗号化された番組データを多重化して送信する送信手段とを設けたものであり、番組データのスクランブルを解くスクランブル鍵が、複数種類の暗号鍵で暗号化されて送信される。

【0041】請求項11に記載の発明は、第2の暗号鍵管理手段が生成管理する第2の種類の暗号鍵の更新期間が、第1の暗号鍵管理手段が生成管理する第1の種類の暗号鍵の更新期間より短くなるようにしたものであり、番組データのスクランブルを解くスクランブル鍵が、更新期間を異にする複数種類の暗号鍵で暗号化されて送信される。

【0042】請求項12に記載の発明は、第2の種類のマスタ鍵を第1の種類のマスタ鍵で暗号化するマスタ鍵暗号化手段を設け、マスタ鍵暗号化手段で暗号化されたマスタ鍵を送信手段を通じて送信するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて各受信装置に配布することができる。

【0043】請求項13に記載の発明は、第1の種類のマスタ鍵を各受信装置ごとに設定し、第2の種類のマスタ鍵を各受信装置に共通に設定するようにしたものであり、蓄積番組の視聴に用いる暗号鍵の暗号化を短時間で済ませることが可能になる。

10

20

30

40

50

【0044】請求項14に記載の発明は、送信装置から放送された番組をリアルタイムで視聴し、または、蓄積した後、再生して視聴する放送システムの受信装置において、暗号化されている第1の種類の暗号鍵を第1の種類のマスタ鍵を用いて復号化する第1の暗号鍵復号手段と、暗号化されている第2の種類の暗号鍵を第2の種類のマスタ鍵を用いて復号化する第2の暗号鍵復号手段と、スクランブル鍵で暗号化された番組データと第2の種類の暗号鍵で暗号化されたスクランブル鍵とを記憶する蓄積手段と、第1の暗号鍵復号手段で復号化された暗号鍵を用いて、現在の受信情報に含まれる暗号化されたスクランブル鍵を復号化する第1のスクランブル鍵復号手段と、第2の暗号鍵復号手段で復号化された暗号鍵を用いて、蓄積手段から読み出した暗号化されているスクランブル鍵を復号化する第2のスクランブル鍵復号手段と、第1のスクランブル鍵復号手段または第2のスクランブル鍵復号手段で復号化されたスクランブル鍵を用いて番組データをデスクランブルするデスクランブラとを設けたものであり、番組をリアルタイム視聴する場合、または、蓄積した番組を再生視聴する場合に、異なる暗号鍵を用いてスクランブル鍵の復号化が行なわれる。

【0045】請求項15に記載の発明は、第2の暗号鍵復号手段で復号化される第2の種類の暗号鍵の更新期間が、第1の暗号鍵復号手段で復号化される第1の種類の暗号鍵の更新期間より短くなるようにしたものであり、更新期間が長い暗号鍵を用いて、番組をリアルタイム視聴するときのスクランブル鍵が復号化され、更新期間が短い暗号鍵を用いて、蓄積した番組を再生視聴するときのスクランブル鍵が復号化される。

【0046】請求項16に記載の発明は、デスクランブラが、番組をリアルタイム視聴するときには、現在受信しているスクランブルされている番組データを、第1のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルし、蓄積された番組を再生して視聴するときには、蓄積手段から読み出したスクランブルされている番組データを、第2のスクランブル鍵復号手段で復号されたスクランブル鍵を用いてデスクランブルするようにしたものであり、番組をリアルタイム視聴するときと、蓄積した番組を再生視聴するときとは、異なる種類の暗号鍵で復号化されたスクランブル鍵を用いて、番組データのスクランブルが解除される。

【0047】請求項17に記載の発明は、暗号化されている第2の種類のマスタ鍵を、第1の種類のマスタ鍵を用いて復号化するマスタ鍵復号手段を設け、マスタ鍵復号手段で復号化されたマスタ鍵を保持するようにしたものであり、蓄積番組視聴用の暗号鍵の復号化に用いるマスタ鍵を、放送を通じて取得することができる。

【0048】請求項18に記載の発明は、第1の種類のマスタ鍵が、各受信装置ごとに設定され、第2の種類のマスタ鍵が、各受信装置に共通に設定されるようにした



ものであり、各受信装置では、蓄積番組の視聴に用いる暗号鍵を、共通のマスタ鍵を使用して復号化する。

【0049】以下、本発明の実施の形態について、図面を用いて説明する。

【0050】(第1の実施形態) 第1の実施形態の蓄積型放送システムでは、番組データにスクランブルを掛けるスクランブル鍵Ksが、更新間隔を異にする2種類の暗号鍵で暗号化される。一方の暗号鍵は、従来の暗号鍵と同様、更新間隔が1年程度であり、この暗号鍵で暗号化されたKsは、受信装置で、番組をリアルタイムで視聴するときに復号化され、番組データのデスクランブルに使用される。この暗号鍵をリアルタイム系暗号鍵と言う。他方の暗号鍵は、番組ごとに更新され、この暗号鍵で暗号化されたKsは、受信装置で、蓄積された番組を視聴するときに復号化され、番組データのデスクランブルに使用される。この暗号鍵を蓄積系暗号鍵と言う。

【0051】リアルタイム系暗号鍵は、受信装置ごとに異なるマスタ鍵で暗号化されて送信される。このリアルタイム系暗号鍵の暗号化に用いるマスタ鍵をリアルタイム系マスタ鍵と言う。一方、蓄積系暗号鍵は、各受信装置に共通のマスタ鍵で暗号化されて送信される。この蓄積系暗号鍵の暗号化に用いるマスタ鍵を蓄積系マスタ鍵と言う。

【0052】このシステムの送信装置は、図1に示すように、番組データ(Data)を生成し管理する番組管理部41と、Dataを暗号化するためのスクランブル鍵Ksを生成し管理するスクランブル鍵管理部42と、リアルタイム系暗号鍵Kw1を、その識別子(Kw1\_ID)と共に生成管理するリアルタイム系暗号鍵管理部43と、リアルタイム系マスタ鍵Km1を、その識別子(Km1\_ID)と共に生成し管理するリアルタイム系マスタ鍵管理部44と、蓄積系暗号鍵Kw2を、その識別子(Kw2\_ID)と共に生成管理する蓄積系暗号鍵管理部45と、蓄積系マスタ鍵Km2を、その識別子(Km2\_ID)と共に生成し管理する蓄積系マスタ鍵管理部46と、DataをKsでスクランブルし、スクランブル化された番組データData'を出力するスクランブラ47と、リアルタイム系暗号鍵Kw1の鍵本体を使ってKsを暗号化し、リアルタイム系暗号化スクランブル鍵Ks'1を出力するリアルタイム系スクランブル鍵暗号部48と、リアルタイム系マスタ鍵Km1の鍵本体を使ってKw1を暗号化し、リアルタイム系暗号化暗号鍵Kw1'を出力するリアルタイム系暗号鍵暗号部49と、蓄積系暗号鍵Kw2の鍵本体を使ってKsを暗号化し、蓄積系暗号化スクランブル鍵Ks'2を出力する蓄積系スクランブル鍵暗号部50と、蓄積系マスタ鍵Km2の鍵本体を使ってKw2を暗号化し、蓄積系暗号化暗号鍵Kw2'を出力する蓄積系暗号鍵暗号部51と、Data'、Ks'1、Kw1'、Ks'2及びKw2'を多重化し、多重化情報として出力する多重化部52と、多重化情報を伝送情報に変換して送信する送信部53とを備えている。

【0053】この送信装置では、番組管理部41で生成されたDataが、スクランブラ47でスクランブル鍵Ksを使ってスクランブルされ、スクランブル化された番組データData'が多重化部52に出力される。

【0054】リアルタイム系暗号鍵管理部43では、生成したリアルタイム系暗号鍵Kw1を識別子Kw1\_IDとともに、Kw1(Kw1\_ID、Kw1本体)の形式で生成管理し、また、蓄積系暗号鍵管理部45では、番組ごとに生成した蓄積系暗号鍵Kw2を識別子Kw2\_IDとともに、Kw2(Kw2\_ID、Kw2本体)の形式で生成管理している。

【0055】リアルタイム系スクランブル鍵暗号部48は、Dataのスクランブルで用いたKsを、リアルタイム系暗号鍵管理部43から出力されたKw1の鍵本体を使って暗号化し、暗号化に用いたKw1の識別子Kw1\_IDを付加して、リアルタイム系暗号化スクランブル鍵をKs'1(Kw1\_ID、Ks'1本体)の形式で多重化部52に出力する。また、蓄積系スクランブル鍵暗号部50は、Ksを蓄積系暗号鍵管理部45から出力されたKw2の鍵本体を使って暗号化し、暗号化に用いたKw2の識別子Kw2\_IDを付加して、蓄積系暗号化スクランブル鍵をKs'2(Kw2\_ID、Ks'2本体)の形式で多重化部52に出力する。

【0056】リアルタイム系マスタ鍵管理部44では、生成したリアルタイム系マスタ鍵を、識別子と共にKm1(Km1\_ID、Km1本体)の形式で管理し、また、蓄積系マスタ鍵管理部46では、生成した蓄積系マスタ鍵を、識別子と共にKm2(Km2\_ID、Km2本体)の形式で管理している。

【0057】リアルタイム系暗号鍵暗号部49は、リアルタイム系暗号鍵の更新時期にKw1(Kw1\_ID、Kw1本体)をKm1の鍵本体を使って暗号化し、暗号化に用いたKm1の識別子Km1\_IDを付加して、リアルタイム系暗号化暗号鍵をKw1'(Km1\_ID、Kw1\_ID'、Kw1'本体)の形式で多重化部52に出力する。

【0058】また、蓄積系暗号鍵暗号部51は、番組の送出に合わせて、Kw2(Kw2\_ID、Kw2本体)をKm2の鍵本体を使って暗号化し、暗号化に用いたKm2の識別子Km2\_IDを付加して、蓄積系暗号化暗号鍵をKw2'(Km2\_ID、Kw2\_ID'、Kw2'本体)の形式で多重化部52に出力する。

【0059】多重化部52は、入力するData'、Ks'1(Kw1\_ID、Ks'1本体)、Ks'2(Kw2\_ID、Ks'2本体)、Kw1'1(Km1\_ID、Kw1\_ID'、Kw1'本体)及びKw2'(Km2\_ID、Kw2\_ID'、Kw2'本体)を多重化して、その多重化情報を送信部53に出力し、送信部53は、それを伝送情報に変換して送信する。

【0060】一方、受信装置は、図2に示すように、受信した伝送情報を多重情報に変換して出力するチューナー61と、チューナー61から出力された多重化情報を暗号化番組データData'、リアルタイム暗号化スクランブル鍵Ks'1、蓄積系暗号化スクランブル鍵Ks'2、リアルタイム系暗号化暗号鍵Kw1'及び蓄積系暗号化暗号鍵Kw2'

に分離して出力する分離部62と、Data'を蓄積する番組データ蓄積部64とKs'2を蓄積するスクランブル鍵蓄積部65とを具備する蓄積媒体76と、分離部62で分離されたData'とKs'2とを対応をとって番組データ蓄積部64及びスクランブル鍵蓄積部65に書き込む書き込み管理部63と、蓄積されているData'とKs'2とを番組データ蓄積部64及びスクランブル鍵蓄積部65から取り出して出力する読み込み管理部66と、各受信装置によって異なるリアルタイム系マスタ鍵Km1を蓄積しているリアルタイム系マスタ鍵蓄積部70と、Km1を使ってKw1'を復号化し、復号化されたKw1を出力するリアルタイム系暗号鍵復号部69と、リアルタイム系暗号鍵復号部69から入力するKw1を蓄積管理するリアルタイム系暗号鍵管理部71と、分離部62から入力するKs'1をリアルタイム系暗号鍵管理部71から取り出したKw1で復号化してKsを出力するリアルタイム系スクランブル鍵復号部72と、各受信装置に共通の蓄積系マスタ鍵Km2を蓄積している蓄積系マスタ鍵蓄積部79と、Km2を使ってKw2'を復号化し、復号化されたKw2を出力する蓄積系暗号鍵復号部78と、蓄積系暗号鍵復号部78から入力するKw2を蓄積管理する蓄積系暗号鍵管理部80と、読み込み管理部66から入力するKs'2を蓄積系暗号鍵管理部80から取り出したKw2で復号化してKsを出力する蓄積系スクランブル鍵復号部81と、リアルタイムで視聴するときは分離部62からData'を選択し、蓄積された番組を視聴するときは読み込み管理部66からData'を選択する番組データ選択部67と、リアルタイムで視聴するときはリアルタイム系スクランブル鍵復号部72で復号化されたKsを選択し、蓄積された番組を視聴するときは蓄積系スクランブル鍵復号部81で復号化されたKsを選択するスクランブル鍵選択部68と、番組データ選択部67から入力するData'をスクランブル鍵選択部68から入力するKsで復号化してDataを出力するデスクランブラ73と、Dataを再生信号にデコードするデコーダ74と、再生信号に基づいて番組表示を行なう表示装置75とを備えている。また、リアルタイム系マスタ鍵蓄積部70、リアルタイム系暗号鍵復号部69、リアルタイム系暗号鍵管理部71、リアルタイム系スクランブル鍵復号部72、蓄積系マスタ鍵蓄積部79、蓄積系暗号鍵復号部78、蓄積系暗号鍵管理部80及び蓄積系スクランブル鍵復号部81はセキュリティモジュール77に設けられており、このセキュリティモジュール77は、放送局から配布され受信装置にセットされる。従って、リアルタイム系マスタ鍵及び蓄積系マスタ鍵は、このセキュリティモジュール77を通じて各受信装置に与えられる。

【0061】この受信装置では、分離部62が、チューナー61から入力する多重化情報を、暗号化番組データData'、リアルタイム系暗号化スクランブル鍵Ks'1(Km1\_ID、Ks'1本体)、蓄積系暗号化スクランブル鍵Ks'2(Kw2\_ID、Ks'2本体)、リアルタイム系暗号化暗号鍵Kw1'(Km1\_ID、Kw1\_ID'、Kw1'本体)及び蓄積系暗号化暗号

鍵Kw2'(Km2\_ID、Kw2\_ID'、Kw2'本体)に分離して出力する。書き込み管理部63は、分離部62から分離されたData'とKs'2とを対応をとって蓄積媒体76の番組データ蓄積部64及びスクランブル鍵蓄積部65に書き込む。

【0062】また、リアルタイム系暗号鍵復号部69は、リアルタイム系マスタ鍵蓄積部70に蓄積されているリアルタイム系マスタ鍵Km1(Km1\_ID、Km1本体)と同一のKm1\_IDをもつリアルタイム系暗号化暗号鍵Kw1'(Km1\_ID、Kw1\_ID'、Kw1'本体)が分離部62から出力されたとき、そのKm1を使ってKw1'を復号化し、復号化したリアルタイム系復号化暗号鍵Kw1(Kw1\_ID、Kw1本体)をリアルタイム系暗号鍵管理部71に出力する。リアルタイム系暗号鍵管理部71は、これを蓄積管理する。

【0063】また、蓄積系暗号鍵復号部78は、蓄積系マスタ鍵蓄積部79に蓄積されている蓄積系マスタ鍵Km2(Km2\_ID、Km2本体)と同一のKm2\_IDをもつ蓄積系暗号化暗号鍵Kw2'(Km2\_ID、Kw2\_ID'、Kw2'本体)が分離部62から出力されたとき、そのKm2を使ってKw2'を復号化し、復号化した蓄積系復号化暗号鍵Kw2(Kw2\_ID、Kw2本体)を蓄積系暗号鍵管理部80に出力する。蓄積系暗号鍵管理部80は、これを蓄積管理する。

【0064】視聴者からリアルタイムの番組視聴が指示された場合には、番組データ選択部67は、分離部62からData'を入手してデスクランブラ73に出力する。また、リアルタイム系スクランブル鍵復号部72は、分離部62からKs'1(Kw1\_ID、Ks'1本体)が入力すると、リアルタイム系暗号鍵管理部71からKs'1と同一のKw1\_IDを持つKw1(Kw1\_ID、Kw1本体)を取り出し、それを使ってKsを復号化する。

【0065】番組データ選択部67と連動するスクランブル鍵選択部68は、リアルタイム系スクランブル鍵復号部72で復号化されたKsを選択してデスクランブラ73に出力する。デスクランブラ73は、このKsを使って番組データ選択部67から入力するData'を復号化し、Dataをデコーダ74に出力する。

【0066】一方、視聴者から蓄積番組の視聴が指示された場合には、読み込み管理部66は、番組データ蓄積部64から、蓄積されている指示された番組のData'を読み出すとともに、そのData'のスクランブルを行なっているKs'2(Kw2\_ID、Ks'2本体)をスクランブル鍵蓄積部65から取り出す。

【0067】番組データ選択部67は、読み込み管理部66からData'を入手してデスクランブラ73に出力する。また、蓄積系スクランブル鍵復号部81は、読み込み管理部66で読み出されたKs'2(Kw2\_ID、Ks'2本体)を入手し、蓄積系暗号鍵管理部80からKs'2と同一のKw2\_IDを持つKw2(Kw2\_ID、Kw2本体)を取り出し、それを使ってKsを復号化する。

【0068】番組データ選択部67と連動するスクランブル鍵選択部68は、蓄積系スクランブル鍵復号部81で復号

化されたKsを選択してデスクランブラ73に出力する。デスクランブラ73は、このKsを使って番組データ選択部67から入力するData'を復号化し、Dataをデコーダ74に出力する。

【0069】このように、この蓄積型放送システムでは、スクランブル鍵Ksが、更新間隔が長いリアルタイム系暗号鍵と、番組ごとに更新される蓄積系暗号鍵とを用いて暗号化され、また、リアルタイム系暗号鍵は、各受信装置ごとに異なるリアルタイム系マスタ鍵で暗号化され、蓄積系暗号鍵は、各受信装置に共通の蓄積系マスタ鍵で暗号化される。

【0070】受信装置では、暗号化されたリアルタイム系暗号鍵をリアルタイム系マスタ鍵で復号化し、今まで保持していた鍵に替えて、新たに復号化したリアルタイム系暗号鍵を保持管理する。また、暗号化された蓄積系暗号鍵を蓄積系マスタ鍵で復号化し、これまで保持していた蓄積系暗号鍵と併せて、新たに復号化した蓄積系暗号鍵を保持管理する。

【0071】また、蓄積媒体には、スクランブル鍵でスクランブルされた番組データと、蓄積系暗号鍵で暗号化されたスクランブル鍵とを蓄積する。

【0072】放送番組をリアルタイムで視聴するときには、保持管理しているリアルタイム系暗号鍵を用いて、リアルタイム系暗号鍵で暗号化されているスクランブル鍵を復号化し、復号化したスクランブル鍵で番組データをデスクランブルする。

【0073】また、蓄積した番組の再生時には、再生する番組に合わせて、保持管理している蓄積系暗号鍵の中から、使用する蓄積系暗号鍵を選択し、その蓄積系暗号鍵で暗号化されているスクランブル鍵を復号化し、復号化したスクランブル鍵で、再生する番組データをデスクランブルする。

【0074】受信装置の蓄積媒体には多数の番組が蓄積されるが、しかし、これらの番組のスクランブルを解くためのスクランブル鍵は、各番組ごとに異なる種類の蓄積系暗号鍵で暗号化されているため、ある番組で用いた蓄積系暗号鍵が不正に解かれたとしても、その他の番組は、不正視聴の対象から免れることができる。

【0075】また、放送送信装置では、暗号化した蓄積系暗号鍵を番組ごとに各受信装置に送信しなければならないが、この暗号化には各受信装置に共通のマスタ鍵を使用しているため、暗号化処理に費やす時間は短くて済み、そのため、更新間隔を短縮することが可能となる。

【0076】なお、ここでは、蓄積系暗号鍵を番組ごとに更新する場合について説明したが、この更新の間隔は、日、週あるいは月単位などで更新するようにしてもよい。また、蓄積系暗号鍵の更新間隔をリアルタイム系暗号鍵の更新間隔と同じにした場合でも、番組をリアルタイム視聴するときの暗号鍵と蓄積した番組を視聴するときの暗号鍵とが異なるために、暗号が不正解読されたと

きの被害の範囲を狭めることができる。

【0077】また、本発明は、番組を自動蓄積する蓄積型の放送システムや、視聴者の選択に基づいて放送番組が蓄積されるシステムなどに適用することができる。

【0078】(第2の実施形態)第2の実施形態の蓄積型放送システムでは、各受信装置に共通に設定する蓄積系マスタ鍵を、放送を通じて各受信装置に配布している。

【0079】このシステムの送信装置は、図3に示すように、リアルタイム系マスタ鍵管理部104で生成されたリアルタイム系マスタ鍵Km1の鍵本体を使って蓄積系マスタ鍵管理部106で生成された蓄積系マスタ鍵Km2を暗号化する蓄積系マスタ鍵暗号部114を備えており、多重化部112は、蓄積系マスタ鍵暗号部114で暗号化された蓄積系暗号化マスタ鍵Km2'(Km1\_ID、Km2\_ID'、Km2'本体)をData'、Ks'1、Ks'2、Km1'及びKm2'とともに多重化し、多重化情報として出力する。その他の構成は第1の実施形態の送信装置(図1)と変わらない。

【0080】一方、このシステムの受信装置は、図4に示すように、リアルタイム系マスタ鍵蓄積部210に蓄積されているリアルタイム系マスタ鍵Km1を使って、分離部202で分離された蓄積系暗号化マスタ鍵Km2'を復号化し、復号化された蓄積系マスタ鍵Km2を出力する蓄積系マスタ鍵復号部222を備えており、蓄積系マスタ鍵復号部222で復号された蓄積系マスタ鍵Km2が、蓄積系マスタ鍵蓄積部219に蓄積される。その他の構成は第1の実施形態の受信装置(図2)と変わらない。

【0081】このシステムでは、蓄積系暗号鍵Km2の暗号化に用いられる各受信装置に共通の蓄積系マスタ鍵Km2が、各受信装置に割り当てたリアルタイム系マスタ鍵Km1を使って暗号化され、それぞれの受信装置に送信される。

【0082】各受信装置では、暗号化されている蓄積系マスタ鍵Km2'を、セキュリティモジュール217で保持しているリアルタイム系マスタ鍵Km1を使って復号化し、蓄積系マスタ鍵蓄積部219に格納する。蓄積系暗号鍵Km2は、この蓄積系マスタ鍵Km2を使って復号化される。

【0083】このように、このシステムでは、リアルタイム系マスタ鍵Km1は、セキュリティモジュール217の配布を通じて各受信装置に与えられ、一方、蓄積系マスタ鍵Km2は、放送を通じて各受信装置に与えられる。そのため、各受信装置に共通に設定する蓄積系マスタ鍵Km2の変更を容易に行なうことができ、この蓄積系マスタ鍵を適宜変更することにより、蓄積系暗号鍵の不正解読を困難にすることができる。

【0084】

【発明の効果】以上の説明から明らかなように、本発明の放送システムでは、番組のリアルタイム視聴の際に用いる暗号鍵と、蓄積した番組を再生視聴する際に用いる

暗号鍵との種類を違えており、また、後者の蓄積系暗号鍵の更新間隔を短く設定しているため、暗号鍵の不正解読による被害を小さい範囲に止めることができる。

【0085】例えば、蓄積系暗号鍵を番組単位で変更する場合には、1つの暗号鍵が不正に解かれても、不正視聴できる番組は1つに限られ、蓄積されている他の番組データの視聴を制限することができる。

【0086】また、本発明の送信装置及び受信装置は、この放送システムを実現することができる。

【図面の簡単な説明】

【図1】本発明の第1の実施形態における放送システムの送信装置の構成を示すブロック図、

【図2】本発明の第1の実施形態における放送システムの受信装置の構成を示すブロック図、

【図3】本発明の第2の実施形態における放送システムの送信装置の構成を示すブロック図、

【図4】本発明の第2の実施形態における放送システムの受信装置の構成を示すブロック図、

【図5】従来の送信装置の構成を示すブロック図、

【図6】従来の受信装置の構成を示すブロック図である。

【符号の説明】

11、41、101 番組管理部

12、42、102 スクランブル鍵管理部

13 暗号鍵管理部

14 マスタ鍵管理部

15、47、107 スクランプラ

16 スクランブル鍵暗号部

17 暗号鍵暗号部

18、52、112 多重化部

19、53、113 送信部

21、61、201 チューナー

22、62、202 分離部

\* 23、63、203 書き込み管理部

24、64、204 番組データ蓄積部

25、65、205 スクランブル鍵蓄積部

26、66、206 読み込み管理部

27、67、207 番組データ選択部

28、68、208 スクランブル鍵選択部

29 暗号鍵復号部

30 マスタ鍵蓄積部

31 暗号鍵管理部

10 32 スクランブル鍵復号部

33、73、213 デスクランブラ

34、74、214 デコーダ

35、75、215 表示装置

36、76、216 蓄積媒体

37、77、217 セキュリティモジュール

43、103 リアルタイム系暗号鍵管理部

44、104 リアルタイム系マスタ鍵管理部

45、105 蓄積系暗号鍵管理部

46、106 蓄積系マスタ鍵管理部

20 48、108 リアルタイム系スクランブル鍵暗号部

49、109 リアルタイム系暗号鍵暗号部

50、110 蓄積系スクランブル鍵暗号部

51、111 蓄積系暗号鍵暗号部

69、209 リアルタイム系暗号鍵復号部

70、210 リアルタイム系マスタ鍵蓄積部

71、211 リアルタイム系暗号鍵管理部

72、212 リアルタイム系スクランブル鍵復号部

78、218 蓄積系暗号鍵復号部

79、219 蓄積系マスタ鍵蓄積部

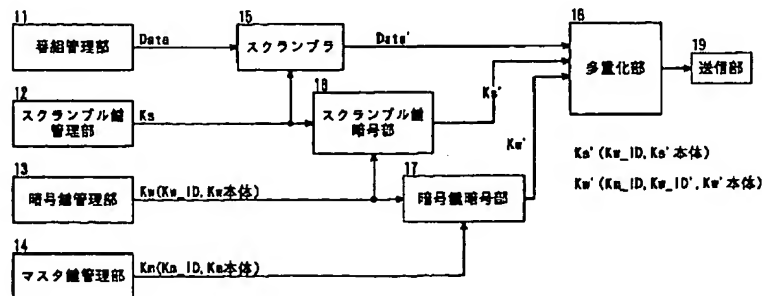
30 80、220 蓄積系暗号鍵管理部

81、221 蓄積系スクランブル鍵復号部

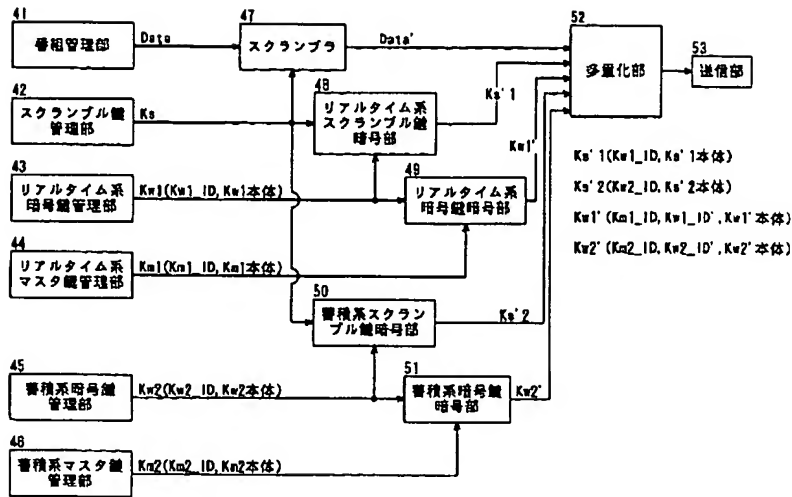
114 蓄積系マスタ鍵暗号部

\* 222 蓄積系マスタ鍵復号部

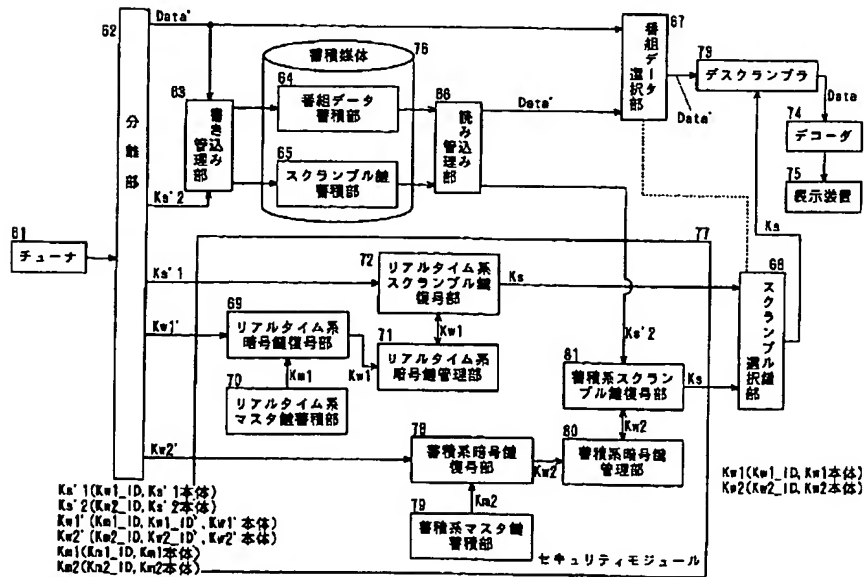
【図5】



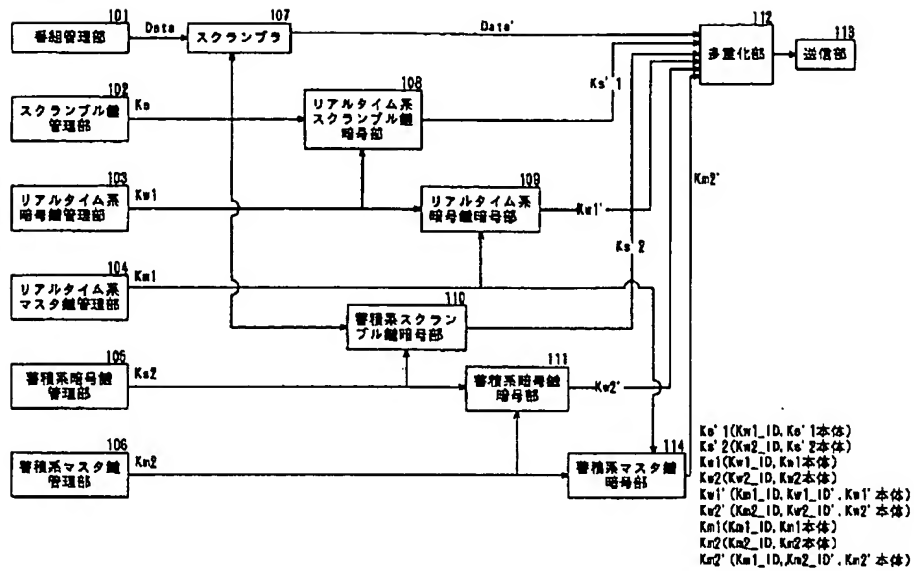
【図1】



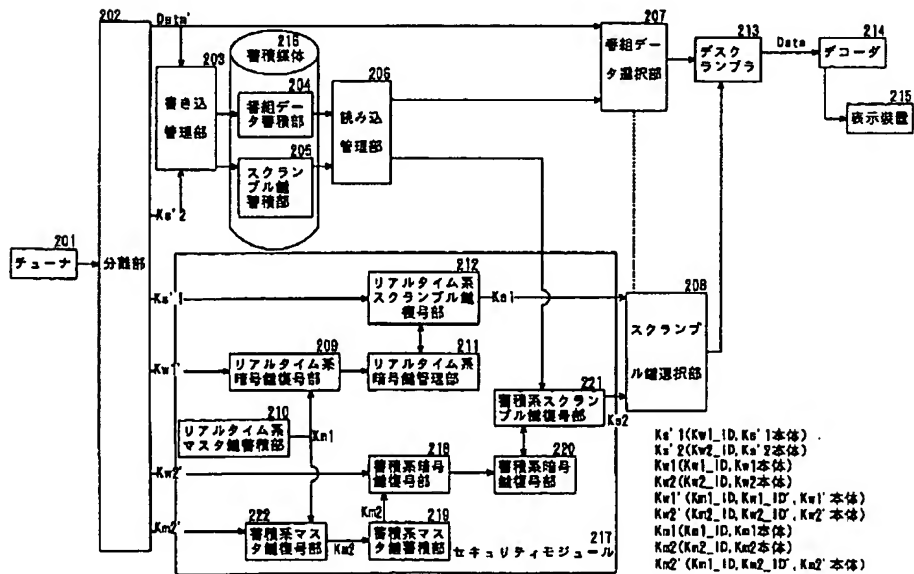
【図2】



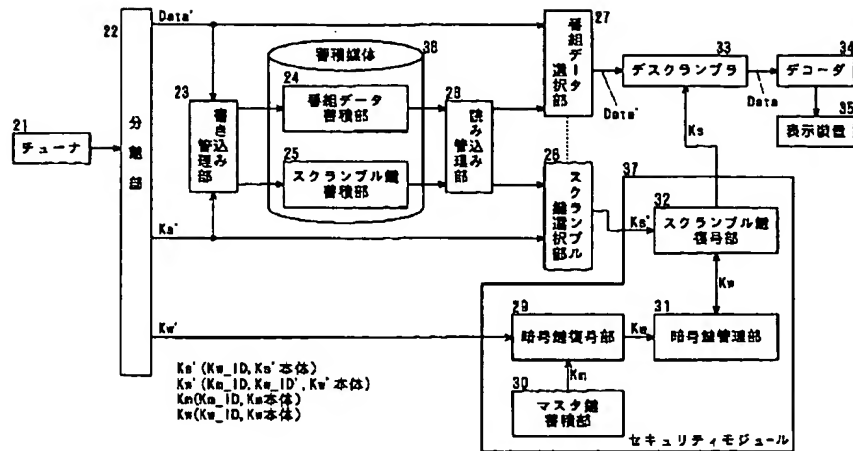
【図3】



【図4】



【図6】



フロントページの続き

(72)発明者 原田 武之助  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

(72)発明者 町田 和弘  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

(72)発明者 片岡 充照  
 大阪府門真市大字門真1006番地 松下電器  
 産業株式会社内

F ターム(参考) 5C064 CA14 CA18 CB01 CB08 CC04  
 CC06  
 5K013 AA01 BA02 BA04 BA05 EA02  
 FA06